UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/715,721	11/17/2003	Sunil K. Srivastava	50325-0855	4990

29989 7590 07/26/2006

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 07/26/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/715,721	SRIVASTAVA, SUNIL K.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 April 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-49* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *1-10 and 27-38* is/are allowed.

6)☒ Claim(s) *11-26 and 39-49* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4/27/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The amendment of 27 April 2006 has been noted and made of record.

2. Claims 1-49 have been presented for examination.

3. Claims 1-10, 27, and 28 have been indicated as allowable.

Information Disclosure Statement

4. The information disclosure statement (IDS) submitted on 27 April 2006 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Response to Arguments

5. Applicant's arguments filed 27 April 2006 have been fully considered but they are not persuasive.

6. In response to applicant's arguments, the recitation "a first network node and two or more other nodes" has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951). Aziz discloses the use of multiple nodes in column 9, lines 26-27.

7. In response to the Applicant's arguments that the cited reference does not disclose a collective public key value of the group, the Examiner respectfully disagrees. As seen in the

citation of column 4, lines 33-44, Aziz discloses the use of SKIP in multicasting, and in particular teaches the use of a group key.

8. Therefore, Aziz discloses at least one node communicating with two or more nodes using multicasting and a group key.

9. In response to the Applicant's arguments that Aziz does not disclose a private key value for the node that is joining the group, the Examiner respectfully disagrees. As taught by Aziz in column 4, lines 33-44, the group key is used in a similar manner that SKIP is used in unicast communications, and as such when a node wants to join the group they must send an encrypted request to the group to join.

10. Therefore, Aziz discloses a key created based on a group key and a key value of the node that is joining the group by at least disclosing SKIP and the Diffie-Hellman protocol in the context of the cited prior art.

11. See further rejections that follow.

Allowable Subject Matter

12. The indicated allowability of claim 26 is withdrawn in view of the 35 U.S.C. 101. Rejections of claim 26 under 35 U.S.C. 101 follows.

13. Reasons for allowance with regards to claims 1-10, 27 and 28 can be found in the office action of 25 January 2006. Claims 29-38 depend from claim 27 and are therefore allowable due to their dependency on a claim that has already been indicated as allowable.

14. Claims 39-49 contain similar language to that of claims 1-10 and 27-38 and therefore would be allowable if rewritten to overcome the 35 U.S.C. 101 rejections set forth below.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

15. Claims 26 and 39-49 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. As provided for on pages 24 and 25 of the specification, a computer-readable medium includes transmission media, including coaxial cables, copper wire, fiber optics, the wires that constitute a bus, and acoustic and light waves that are generated during radio wave and infrared data communications. The Office's current position is that claims involving signals encoded with functional descriptive material do not fall within any of the categories of patentable subject matter set forth in 35 U.S.C. § 101, and such claims are therefore ineligible for patent protection. *See* 1300 OG 142 (November 22, 2005) (in particular, see Annex IV(c)).

Claim Rejections

16. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

17. Claims 11-15, 17-20, and 22-25 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 5,668,877 to Aziz, hereinafter Aziz.

18. As per claim 11, Aziz teaches a method for establishing a secure communication session among a first node of a network and one or more other nodes that joined in a first network communication entity, using a group shared secret key value, each of the nodes having a private key value associated therewith, the method comprising the computer-implemented steps of:

communicating a first public key value from a first node that is joining the first network communication entity to each other node that is currently within the first network communication entity (column 2, lines 20-44, column 8, line 30 to column 9, line 67);

receiving a collective public key value that is shared by each other node in the first network communication entity and that is based on private key values associated with each other node in the network communication entity (column 2, lines 20-44, column 4, lines 33-53, column 8, line 30 to column 9, line 67);

creating the group shared secret key value based on the collective public key value and the private key value associated with the first node (column 2, lines 20-44, column 4, lines 33-53, column 8, line 30 to column 9, line 67); and

joining the first node to a second network communication entity that includes the first network communication entity and the first node and that uses secure communication with messages that are encrypted using the group shared secret key value (column 4, lines 33-53, column 14, line 3 to column 16, line 58)

19. Regarding claim 12, Aziz teaches wherein joining the first node to a second network communication entity includes the step of communicating the first private key value to the second node and to the third node using messages encrypted using the shared secret key value (column 4, lines 33-53, column 8, line 30 to column 9, line 67, column 14, line 3 to column 16, line 58, i.e. acquiring a new member to join group).

20. Regarding claim 13, Aziz teaches wherein creating and storing a shared secret key value further comprises creating and storing the shared secret key based upon how many times each node of the second network communication entity has participated in formation of any such entity and based upon each private number of each node in the second network communication entity (column 3, lines 9-50).

21. Regarding claim 14, Aziz teaches further comprising the step of creating and storing a subsequent shared secret key for use by the first network communication entity and the third node to enable the third node to independently compute the group shared secret key (column 4, lines 33-53, column 8, line 30 to column 9, line 67, column 14, line 3 to column 16, line 58).

22. With regards to claim 15, Aziz teaches wherein creating and storing the subsequent shared secret key comprises creating and storing the subsequent shared secret key, k, according to the relation

$$k = p^{(a*x)(b*y)(c*z)} \bmod (q)$$

where p = a random number, q = a prime number, a = the first private key value, b = the second private key value, c = a private key value of the third node, x = a number of times the first node has participated in entity formation, y = a number of times the second node has participated in entity formation, and z = a number of times the third node has participated in entity formation (column 3, lines 10-50, column 10, lines 3-40).

23. Regarding claim 17, Aziz teaches wherein the step of joining the first node to a second network communication entity further comprises creating and storing a subsequent collective

public key based upon the collective public key value and the first public key value of the first node (column 4, lines 33-53, column 8, line 30 to column 9, line 67, column 14, line 3 to column 16, line 58).

24. Regarding claim 18, Aziz teaches wherein the step of joining the first node to a second network communication entity further comprises receiving the collective public key from one of the nodes of the first network communication entity that was the first node to join the first network communication entity (column 4, lines 33-53, column 8, line 30 to column 9, line 67, column 14, line 3 to column 16, line 58).

25. Regarding claim 19, Aziz teaches wherein creating and storing an initial shared secret key for the first node and second node comprises creating and storing an initial shared public key "AB" according to the relation

$$AB = k_{ab}^{ab} \bmod (q) = p^{(ab)(ab)} \bmod (q)$$

wherein k = the initial shared secret key value, a = the first private key value, b = the second private key value, p is a base value, and q is a randomly generated prime number value (column 3, lines 10-50, column 10, lines 3-40).

26. As per claim 20, Aziz discloses a method for exchanging cryptographic keys, the method comprising:

forming a multicast group initially comprising a first node and a second node, the first node generating a first private value, the second node generating a second private value, wherein

the initial multicast group exchanges the first private value and the second private value with ht second node and the first node, respectively, using a shard secret key, the multicast group generating a common public key (column 2, lines 20-44, column 4, lines 33-53, column 8, line 30 to column 9, line 67); and

joining the multicast group by a new node, the new node generating a new private value and a corresponding public key, the step of joining includes:

sending the common public key of the multicast group by a member of the multicast group by a member of the multicast group to the new node; tracking a number of times each node in the multicast group participates in the step of joining; computing a new shared secret key by the new node based upon the common public key of the multicast group and the new private value; publishing the public key of the new node; and computing the new shared secret key by each member of the multicast group based upon the public key of the new node, the private values of each member, and the number of times each node in the multicast group participates in the step of joining (column 4, lines 33-53, column 14, line 3 to column 16, line 58).

27. Concerning claim 22, Aziz discloses wherein the step of joining the first node to a second network communication entity further comprises determining which one of the nodes of the first network communication entity is designated to transfer the collective public key based upon order of entry into the formed entity (column 4, lines 33-53, column 14, line 3 to column 16, line 58).

28. Concerning claim 23, Aziz teaches wherein the step of joining the first node to a second network communication entity further comprises determining which one of the nodes of the first network communication entity is designated to transfer the collective public key based upon a predetermined metric (column 12, line 59 to column 13, line 67).

29. Regarding claim 24, Aziz teaches wherein the plurality of nodes communicate over a packet switched network that supports, in part, Internet Protocol (column 2, lines 65-67).

30. Regarding claim 25, Aziz teaches wherein the first node, the second node, and the new node are authenticated by a distributed directory (column 4, lines 33-57).

31. Claims 16 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aziz in view of U.S. Patent No. 6,629,243 to Kleinman et al, hereinafter Kleinman.

32. Regarding claims 16 and 21, Aziz does not teach wherein the step of communicating the first public key value of the first node to the first network communication entity by storing the first key value in a key distribution center.

33. Kleinman discloses wherein the step of communicating the first public key value of the first node to the first network communication entity by storing the first key value in a key distribution center (column 2, lines 60-67).

34. It would have been obvious to one of ordinary skill in the art at the time the invention was made to distribute the keys via a key distribution center, since Kleinman states at column 2, lines 51-59 that such a modification would ensure the safe and secure distribution of the keys to the respective members of the group.

Conclusion

35. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

36. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

37. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

38. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

39. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

CLF

Christian LaForgia
Patent Examiner
Art Unit 2131

clf

7/21/06